

IN THE TITLE:

OK Change the title from "SYSTEM FOR TRACKING END-USER ELECTRONIC CONTENT USAGE" to --MULTIMEDIA PLAYER TOOLKIT FOR ELECTRONIC CONTENT DELIVERY--.

IN THE SPECIFICATION:

OK As requested in paragraph 6 of the accompanying request for filing a divisional application, please amend the specification by inserting before the first line --This is a divisional of application Serial No. 09/177,096, filed October 22, 1998, now ____, which is a continuation-in-part of application Serial No. 09/133,519, filed August 13, 1998, now ____. The entire disclosure of prior application Serial No. 09/177,096 is herein incorporated by reference.--

Additionally, please delete from the table on page 1 the row beginning with "SE9-98-007".

IN THE ABSTRACT:

Please substitute the attached substitute abstract for the abstract that was originally filed.

IN THE CLAIMS:

As requested in paragraph 5 of the accompanying request for filing a divisional application, please cancel claims 2-44.

Please also cancel claim 1.

Please add new claims 45-82 as follows:

B 1
--45. A computer readable medium comprising program instructions for a software toolkit containing a collection of data structures and subroutines for developing an application for playing digital content, the program instructions comprising instructions for:
acquiring metadata which has been previously associated with content; and

rendering the metadata on an end-user's system.--

- 46. The computer readable medium according to claim 45, further comprising instructions for:
- receiving previously encrypted content encrypted with an encrypted key from an external source;
 - creating an encrypted container using an encrypting key from a clearing house;
 - transferring the encrypted container to the clearing house for authentication of permission to decrypt the content; and
 - receiving, from the clearing house, a decrypting key for decrypting at least part of the previously encrypted content as permitted.--
- 47. The computer readable medium according to claim 46, further comprising an instruction for:
- playing at least part of the previously encrypted content by decrypting the encrypted content with a decryption key from the clearing house.--
- 48. The computer readable medium according to claim 46, further comprising the instructions for:
- transferring a local encrypting key from the application to the clearing house; and
 - receiving from the clearing house a decrypting key which has been encrypted using the local encrypting key from the application.--
- 49. The computer readable medium according to claim 45, further comprising an instruction for:
- creating user controls for controlling the rendering of the metadata.--
- 50. The computer readable medium according to claim 48, further comprising an instruction for:

creating user controls for controlling the playing of the content.--

--51. The computer readable medium according to claim 47, further including instructions for:
decrypting the previously encrypted content with a decryption key: and
reencrypting the content with a second encrypting key.--

--52. The computer readable medium according to claim 51, further including instructions for
creating a tamper resistant environment for deterring unauthorized access to the
instructions for decrypting and reencrypting the content.--

53. A computer readable medium containing program instructions for a software toolkit
containing a collection of data structures and subroutines for developing an application for
playing digital content data, the program instructions comprising instructions for:
receiving previously encrypted content data encrypted with an encryption key from an
external source;
storing the previously encrypted content data in a library;
selecting one or more encrypted content data from the library to play; and
decrypting each content data selected to be played with its unique decryption key,
wherein the decrypting is performed in a tamper-resistant subroutine for deterring unauthorized
access to the instructions for decrypting the content data and for deterring unauthorized access to
the decryption key.--

--54. The computer readable medium according to claim 53, further including instructions for:
decrypting the received previously encrypted content data prior to storage in the library;
reencrypting the decrypted received content data with a local encrypting key
wherein the decrypting and reencrypting instructions are performed in the tamper resistance
subroutine.--

121098-04409802

Sub
01

Sub
01 --55. The computer readable medium according to claim 54, wherein the instruction for reencrypting the decrypted received content data utilizes a unique local decrypting key for each content data prior to storage in the library.

--56. The computer readable medium according to claim 55, further comprising instruction for: reencrypting each unique local decrypting key with a common local encryption key.

--57. The computer readable medium according to claim 56, further including instructions for: storing the unique local decrypting key in several distinct parts throughout an information processing system.--

--58. The computer readable medium according to claim 56, further including instructions for: storing the common local decrypting key in several distinct parts throughout an information processing system.--

--59. The computer readable medium according to claim 53, further including instructions for: creating play-lists for playing one or more content data and playing the content data in each play list.--

--60. The computer readable medium according to claim 59, further including instructions for: naming each play-list created; and storing the named play list for playing the content data in each play list at a later time.--

--61. The computer readable medium according to claim 59, further including instructions for: sorting each play-list in response to a user request.--

--62. The computer readable medium according to claim 53, further including instructions for: playing each content data selected to be played; and displaying the metadata associated with the content data.--

090727-121099

receiving from the clearing house a decrypting key which has been encrypted using the local encrypting/key from the application.

--69. The method according to claim 64, further comprising the step of:
creating user controls for controlling the rendering of the metadata.--

--70. The method according to claim 66, further comprising the step of:
creating user controls for controlling the playing of the content.--

--71. The method according to claim 65, further comprising the steps of:
decrypting the previously encrypted content with a decryption key;
reencrypting the content with a second encrypting key.--

--72. The method according to claim 71, further comprising the step of:
creating a tamper resistant environment for deterring unauthorized access to the
instructions for decrypting and reencrypting the content.--

SECRET 0460260
549-73
02
A method for providing a collection of data structures and subroutines for developing an application for playing digital content data, the method comprising the steps of:
receiving previously encrypted content data encrypted with an encrypted key from an external source;
storing the previously encrypted content data in a library;
selecting one or more encrypted content data from the library to play; and
decrypting each content data selected to be played with its unique decrypting key,
wherein the decrypting is performed in a tamper-resistant subroutine for deterring unauthorized access to the instructions for decrypting the content data and for deterring unauthorized access to the decrypting key.--

--74. The method according to claim 73, further comprising the step of:

Sub
02

decrypting the received previously encrypted content data prior to storage in the library;
reencrypting the decrypted received content data with a local encryption key
wherein the decrypting and reencrypting instructions are performed in the tamper resistance
subroutine.--

--75. The method according to claim 74, wherein the step of reencrypting the decrypted
received content data utilizes a unique local encryption key for each content data prior to storage
in the library.

--76. The method according to claim 74, further comprising the step of:
reencrypting each unique local encryption key with a common local encryption key.--

--77. The method according to claim 75, further comprising the step of:
storing the unique local encryption key in several distinct parts throughout an information
processing system.--

--78. The method according to claim 74, further comprising the step of:
storing the common local encryption key in several distinct parts throughout an
information processing system.--

--79. The method according to claim 73, further comprising the steps of:
creating play-lists for playing one or more content data and
playing the content data in each play list.--

--80. The method according to claim 79, further comprising the steps of:
naming each play-list created; and
storing the named play list for playing the content data in each play list at a later time.--

--81. The method according to claim 79, further comprising the step of

09209440-121098
B60727-044502B

sorting each play-list in response to a user request.--

- 82. The method according to claim 76, further comprising the steps of:
playing each content data selected to be played; and
displaying the metadata associated with the content data.--
-

850727-04750260